(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 2 316 190 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
29.06.2016 Bulletin 2016/26

(21) Application number: **09808406.4**

(22) Date of filing: **20.08.2009**

(51) Int Cl.:
G06F 21/62 *(2013.01)* ***H04L 29/08*** *(2006.01)*

(86) International application number:
PCT/KR2009/004649

(87) International publication number:
WO 2010/021502 (25.02.2010 Gazette 2010/08)

(54) METHOD AND APPARATUS FOR PROTECTING PERSONAL INFORMATION IN A HOME NETWORK

VERFAHREN UND VORRICHTUNG ZUM SCHUTZ PERSÖNLICHER INFORMATIONEN IN EINEM HEIMNETZWERK

PROCÉDÉ ET APPAREIL POUR LA PROTECTION DES INFORMATIONS PERSONNELLES SUR UN RÉSEAU DOMESTIQUE

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO SE SI SK SM TR

(30) Priority: **20.08.2008 KR 20080081421**
03.04.2009 KR 20090029149
14.08.2009 KR 20090075449

(43) Date of publication of application:
04.05.2011 Bulletin 2011/18

(73) Proprietor: **Samsung Electronics Co., Ltd.**
Suwon-si, Gyeonggi-do, 443-742 (KR)

(72) Inventors:
- **HAN, Se-Hee**
  Seoul 138-224 (KR)
- **LEE, Joo-Yeol**
  Seoul 150-070 (KR)
- **JUNG, Dong-Shin**
  Suwon-si
  Gyeonggi-do 443-751 (KR)
- **MAENG, Je-Young**
  Suwon-si
  Gyeonggi-do 443-470 (KR)
- **FENG, Fei Fei**
  Suwon-si
  Gyeonggi-do 443-725 (KR)

(74) Representative: **Gover, Richard Paul et al**
HGF Limited
Saviour House
9 St Saviourgate
York YO1 8NQ (GB)

(56) References cited:
US-A1- 2003 219 127 **US-A1- 2004 064 575**
US-A1- 2004 158 634 **US-A1- 2005 074 018**
US-A1- 2006 004 924 **US-A1- 2006 184 530**
US-A1- 2006 209 768 **US-A1- 2008 066 145**

- **JAMMES F ET AL: "Service-Oriented Device Communications Using the Devices Profile for Web services", ADVANCED INFORMATION NETWORKING AND APPLICATIONS WORKSHOPS, 2007, AINAW '07. 21ST INTERNATIONAL CONFERENCE ON, IEEE, PISCATAWAY, NJ, USA, 21 May 2007 (2007-05-21), pages 947-955, XP031334642, ISBN: 978-0-7695-2847-2**
- **FENG WANG ET AL: "Services and Policies for Care At Home", PERVASIVE HEALTH CONFERENCE AND WORKSHOPS, 2006, IEEE, PI, 1 November 2006 (2006-11-01), pages 1-10, XP031089347, ISBN: 978-1-4244-1085-9**
- **RAMAKRISHNA V ET AL: "Negotiating Agreements Using Policies in Ubiquitous Computing Scenarios", SERVICE-ORIENTED COMPUTING AND APPLICATIONS, 2007. SOCA '07. IEEE INTE RNATIONAL CONFERENCE ON, IEEE, PI, 1 June 2007 (2007-06-01), pages 180-190, XP031116782, ISBN: 978-0-7695-2861-8**

Printed by Jouve, 75001 PARIS (FR)

(Cont. next page)

- **BRENT A MILLER ET AL: "Home Networking with Universal Plug and Play", IEEE COMMUNICATIONS MAGAZINE, IEEE SERVICE CENTER, PISCATAWAY, US, vol. 39, no. 12, 1 December 2001 (2001-12-01), pages 104-109, XP011091867, ISSN: 0163-6804**

Description

Technical Field

[0001] The present invention relates generally to Universal Plug and Play (UPnP), or a middleware protocol for home networking, and more particularly, to a method and an apparatus for protecting personal information of users in a UPnP-based home network.

Background Art

[0002] In general, a home network, which consists of Internet Protocol (IP)-based private networks, connects and controls various types of devices used in a home, such as Personal Computers (PCs), intelligent products and wireless devices. These devices are connected to a single network through a common virtual computing environment called "middleware".

[0003] The term "middleware" refers to software that connects various digital devices on a peer-to-peer basis and enables communication between the devices. Various types of technology, such as Home AV Interoperability (HAVI), UPnP, Java Intelligent Network Infra-structure (JINI), and Home Wide Web (HWW), have been proposed as middleware.

[0004] Since the addition of Plug and Play (PnP) functions to current operating systems, it has been very easy to install and set peripheral devices of PCs. UPnP, which has evolved from PnP, enables various home appliances and network devices, such as network printers and Internet gates, to perform networking, especially home networking. UPnP provides convenient functions to the entire network based on Internet standard technologies, such as Transmission Control Protocol/Internet Protocol (TCP/IP), Hyper Text Transfer Protocol (HTTP), and extensible Markup Language (XML).

[0005] A UPnP network consists of Controlled Devices (CDs), which are connected to and controlled by an IP-based home network. The UPnP is also consisted of Control Points (CPs) for controlling the CDs. The UPnP network performs communication between the CPs and the CDs through the use of a UPnP protocol stack structure that includes Internet protocols such as TCP/IP and HTTP, and technologies such as XML and Simple Object Access Protocol (SOAP).

[0006] In a first addressing step of UPnP communication, a CP and a CD have their own individual IP addresses. Upon joining the network, the CD fetches its IP address using a Dynamic Host Configuration Protocol (DHCP), or it is assigned an IP address using automatic IP addressing if there is no DHCP server in the network.

[0007] In a second discovery step, the CP searches for the CD, or the CD advertises its location. The discovery step is performed using a Simple Service Discovery Protocol (SSDP). If the CD is added to the network, the CD delivers an SSDP alive message to the network through IP multicasting. The CP can determine the presence/absence of the CD through the reception of the alive message. When the CP newly joins the network, the CP multicasts an SSDP Multicast-search (M-search) message to the network. All of the CDs, which checked the M-search message, send M-search response messages containing their own information to the CP.

[0008] In a third description step, the CP checks the description content of the CD. When the CP wants the CD after checking the response message, the CP may send to the CD a request for detailed information related to the CD. The CD, which has received the request, sends its information in an XML document.

[0009] In a fourth control step, the CP operates the CD by controlling a function of the CD. When the CP intends to control an arbitrary CD, the CP sends a desired service to the CD using SOAP, based on the detailed information related to the CD. SOAP is a protocol that is written on HTTP by XML for the purpose of invoking (or calling) a remote function.

[0010] a fifth event step, the CP receives an event change of the CD. The CP sends a subscribe request for a relevant event to the CD when the CP desires to receive an event message from the CD. If the subscription is successful, the CD sends an event message to the CP using General Event Notification Architecture (GENA).

[0011] In a sixth presentation step, the CP presents a state of the CD using a Hyper Text Markup Language (HTML) of the CD.

[0012] FIG. 1 is a diagram illustrating device discovery and action execution in a conventional UPnP network system.

[0013] Referring to FIG. 1, in step 110, a CP 101 discovers or searches for a CD 102, or the CD 102 advertises its location. In step 120, the CP 101 sends an action request to the CD 102. In step 130, the CD 102 performs an action corresponding to the received action request. In step 140, the CD 102 provides a response to the CP 101 with the action result. More specifically, the CD 102 performs the requested action, and transmits the execution result for the action or an error message to the CP 101.

[0014] Based on the above-described basic UPnP control method, a UPnP CD can provide various services (or functions) to the CP. For example, based on the basic UPnP control method, a UPnP CP can control the UPnP CD in which Audio/Visual (A/V) content is stored, so that the A/V content can be played back in other UPnP CDs. When the UPnP CD is a gateway, the UPnP CP can change and set an IP address band and addresses of a subnet and a gateway, to be assigned to the devices in the home, by controlling the UPnP gateway, or the CD.

[0015] FIG. 2 is a diagram illustrating an event notification in a conventional UPnP network system.

[0016] Referring to FIG. 2, in step 210, a CP (or display device) 201 searches for a CD (or mobile phone) 202, or the CD 202 advertises its location. In step 220, the CP 201 sends a request for event reception/registration (or subscribes) to the CD 202. Upon receipt of the subscribe

request, the CD 202 assigns a Subscribe ID (SID) in step 230, and delivers the assigned SID to the CP 201 in step 240. If an event occurs in the CD 202 in step 250, the CD 202 delivers the event to the CP 201 in step 260. If there is a change in an event-related state variable among state variables defined in association with respective UPnP services, the CD 202 delivers the relevant event to the CP 201 that sent the subscribe request.

[0017] FIG. 3 is a diagram illustrating a subscribe request message from a CP to a CD in a conventional UPnP network system. Methods and headers of the subscribe message follow the format defined in UPnP Device Architecture.

[0018] A UPnP telephony service can be provided to the CD as a UPnP service based on the above-described technology. In the telephony service, if an incoming call or a text message is received at a mobile terminal (or CD), the mobile terminal notifies the pertinent event to a display device (or CP). If the display device requests the received call information or text message information, the mobile terminal can provide the call information or text message information in response to the request.

[0019] However, because call information or text message information is delivered to the CP, event information from the CD to the CP may include a user's personal information. The result values for a UPnP action requested by the CP from the CD may also include a user's personal information stored in the CD. Thus, personal information of users enjoying the UPnP service may be leaked out.

[0020] Jammes F et al: "Service-Oriented Device Communications Using the Devices Profile for Web services", 21st International Conference on Advanced Information Networking and Applications Workshops, 2007, AINAW '07, IEEE, Piscataway, NJ, USA, 21 May 2007. This document outlines the benefits of adopting service-oriented architectures at the level of the communications between resource-constrained embedded devices, in particular for industrial device networks. If focuses on the usage of the Devices Profile for Web Services (DPWS) as the underpinning of such "smart device" architectures and discusses an implementation thereof.

[0021] US-2005/074018A1 discloses a universal plug and play (UPnP) device which makes itself known through a set of processes-discovery, description, control, eventing, and presentation. Following discovery of a UPnP device, an entity can learn more about the device and its capabilities by retrieving the device's description. The description includes vendor-specific manufacturer information like the model name and number, serial number, manufacturer name, URLs to vendor-specific Web sites, etc. The description also includes a list of any embedded devices or services, as well as URLs for control, eventing, and presentation. The description is written by a vendor, and is usually based on a device template produced by a UPnP forum working committee. The template is derived from a template language that is used to define elements to describe the device and any services supported by the device.; The template language is written using an XML-based syntax that organizes and structures the elements.

[0022] US-2004/064575-A1 discloses a method including matching a data transmission characteristic of a first application on a first network device and of a second application on a second network device, requesting a prioritized data transfer between the first and second applications from a policy manager application, determining whether to approve the requested prioritized data transfer based upon a set of policy rules, and transferring data between the first and second application with preferential treatment.

[0023] Feng Wang et al: "Services and Policies for Care At Home", Pervasive Health Conference and Workshops, 2006, IEEE, PI, 1 November 2006. This document outlines desirable characteristics of care services to be delivered to aging users in their own homes. The OSGi is described as being particularly suitable for developing home care services. Service discovery is enhanced through ontologies that achieve greater flexibility and precision in service description.

Disclosure of Invention

Technical Problem

[0024] Embodiments of the present invention have been made to address at least the above problems and/or disadvantages and to provide at least the advantages described below. Accordingly, an aim of embodiments of the present invention is to provide a personal information protection method and apparatus for preventing leakage of a user's personal information, which may occur during execution of a UPnP service in a UPnP home network.

Technical Solution

[0025] Another aim of embodiments of the present invention is to provide a UPnP-based service, a series of an action invocation method, a controlled device control method and a controlled device-to-control point event method, needed to provide the UPnP service, and a controlled device and a control point device for the same.

[0026] According to a first aspect of the present invention there is provided a method for protecting personal information in a home network, the method comprising the steps of: receiving, by a controlled device, a subscribe request for a service of the controlled device, from a control point; accepting, by the controlled device, the subscribe request; receiving, by the controlled device, information about the control point from the control point; and performing, by the controlled device, event information delivery to the control point according to a policy when an event occurs in the controlled device; wherein the method is characterized in that it further comprises the steps of: transmitting, by the controlled device, the infor-

mation about the control point to a policy manager; and receiving, by the controlled device, a policy for event information delivery to the control point, which is generated by the policy manager based on the information about the control point; wherein the step of performing, by the controlled device, event information delivery to the control point is in accordance with the policy received from the policy manager, wherein the policy manager generates the policy for event information delivery by setting event delivery conditions based on user input, said event delivery conditions prescribing whether at least one of delivery, authentication and encryption is to be applied.

[0027] According to a second aspect of the present invention there is provided a controlled device for protecting personal information in a home network, the controlled device comprising: a receiver; an event manager; and a transmitter; wherein the receiver is arranged to receive information over the home network including a subscribe request for a service of the controlled device from a control point; wherein the controlled device is arranged to accept the subscribe request; wherein the receiver is further arranged to receive information about the control point from the control point; wherein the event manager is arranged to determine when an event occurs and to control event information delivery to the control point according to a policy; and wherein the transmitter is arranged to transmit the event information to the control point; wherein the controlled device is characterized in that: the transmitter is further arranged to transmit the information about the control point to a policy manager; the receiver is further arranged to receive a policy for event information delivery to the control point, which is generated by a policy manager based on the information about the control point; and the event manager is further arranged to control event information delivery to the control point according to the policy received from the policy manager, wherein the policy manager generates the policy for event information delivery by setting event delivery conditions based on user input, said event delivery conditions prescribing whether at least one of delivery, authentication and encryption is to be applied.

Advantageous Effects

[0028] As is apparent from the foregoing description, according to embodiments of the present invention, when an event occurs in a service that a UPnP home network system provides to a CD, the CD performs event notification based on a set policy, without delivering the event to all CP devices that sent a subscribe request to the service. In addition, based on the set policy, the CD may request authentication or encrypt detailed event information with personal information, which is requested by the CP.

[0029] Accordingly, the present invention prevents privacy information, which is stored in the CD or provided by the CD through a service, from being included in the event information, making it possible to protect the user's personal information.

Brief Description of Drawings

[0030] The above and other aspects, features and advantages of the present invention will be more apparent from the following detailed description when taken in conjunction with the accompanying drawings, in which:

FIG. 1 is a diagram illustrating device discovery and action execution in a conventional UPnP network system;
FIG. 2 is a diagram illustrates an event notification operation in a conventional UPnP network system;
FIG. 3 is a subscribe request message from a CP to a CD in a conventional UPnP network system;
FIG. 4 is a diagram illustrating a session generation operation for event delivery during a UPnP service, according to an embodiment of the present invention;
FIG. 5 is a diagram illustrating a policy-based event delivery operation during a UPnP service, according to an embodiment of the present invention;
FIG. 6 is a diagram illustrating a filter-based event delivery operation during a UPnP service, according to another embodiment of the present invention;
FIG. 7 is a diagram illustrating a detailed event delivery operation during a UPnP service, according to an embodiment of the present invention;
FIG. 8 is a diagram illustrating a detailed event delivery operation when encryption parameter negotiation is not performed, according to an embodiment of the present invention;
FIG. 9 is a subscribe request message in which information on a CP is included in a policy-based event delivery operation during a UPnP service, according to an embodiment of the present invention;
FIG. 10 is a block diagram of a device for protecting personal information during a UPnP service, according to an embodiment of the present invention; and
FIG. 11 is a filter list in a filter-based event delivery operation during a UPnP service, according to another embodiment of the present invention.

Mode for the Invention

[0031] Embodiments of the invention are described in detail with reference to the accompanying drawings. The same or similar components may be designated by the same or similar reference numerals although they are illustrated in different drawings. Detailed descriptions of constructions or processes known in the art may be omitted to avoid obscuring the subject matter of the present invention.

[0032] FIG. 4 is a diagram illustrating a session generation operation for event delivery during a UPnP service, according to an embodiment of the present invention. The scheme illustrated in FIG. 4 maps SIDs and device

information to subscribe requests based on session authentication. The event scheme shown in FIG. 4 causes a CP or a user issuing a subscribe request for an event of a service provided by a CD to be subject to authentication. The CD can acquire information about a device or a user as authentication results on the device or the user, and maps the acquired information to an event session.

[0033] Referring to FIG. 4, if a CP 401 sends a subscribe request to a CD 402 in step 405, the CD 402 sends an error message in response to the request in step 410. This error message is not defined in the existing UPnP Device Architecture standard, and its error code is defined as '413' in this embodiment of the present invention. Such an error code value notifies the CP 401 that sent the subscribe request of a need for an authentication process. A device supporting the authentication in the CP 401 performs a series of authentication procedures. The detailed authentication procedure and message format are defined in the UPnP Device Protection standard. In step 415, the CP 401 and the CD 402 generate a Transport Layer Security (TLS) session using a self-signed certificate for channel protection between the two devices. In step 420, in order to authenticate the CP 401, an authentication procedure is performed using an introduction protocol, such as Wi-fi Protected Setup (WPS) and Transport Layer Security Pre-Shared Key (TLS-PSK). After the generation of the TLS session, the CP 401 sends a role request to the CD 402 in step 425. When the CP 401 needs another role, the CP 401 may perform login in step 430, and when the CP 401 changes its role, the CP 401 may change an Access Control List (ACL) in step 435.

[0034] After the authentication process, the CP 401 sends a subscribe request to the CD 402 in step 440, and the CD 402 accepts the subscribe request using an accept message (hereinafter referred to as an "HTTP 200 OK message") in step 445. When sending the subscribe request in step 440, the CP 401 may deliver port information of a callback Uniform Resource Locator (URL) to the CD 402 along with the subscribe request. Thereafter, if an event occurs in a service of the CD 402 in step 450, a TLS session is generated, a single time at first, in step 455. During the TLS session generation, the CD 402 generates the TLS session on the port of the callback URL that the CP 401 delivered along with the subscribe request. The CD 402 delivers the event to the CP 401 in step 460.

[0035] During the TLS session generation, the CD 402 may reuse the TLS session that it used during the authentication procedure.

[0036] FIG. 5 illustrates a policy-based event delivery operation during a UPnP service, according to an embodiment of the present invention. In this embodiment of the present invention a mobile phone serves as a CD, a display device serves as a CP, and the policy-based event delivery operation is performed during occurrence of a call event in a UPnP telephony service.

[0037] Referring to FIG. 5, in step 505, a CP 501 discovers a CD 502, or the CD 502 advertises its location. In step 510, the CP 501 sends a subscribe request to a telephony service of the CD 502. In step 515, the CD 502 assigns an SID to the CP 501, accepting the subscribe request from the CP 501. In step 520, the CD 502 returns the assigned SID to the CP 501. In step 525, the CP 501 maps its Universally Unique Identifier (UUID) and friendly name information to the assigned SID, and the mapped information is stored in the CD 502. This is performed by a SOAP action such as 'Set-FriendlyName()'.

[0038] Mapping information of the CP 501 to the assigned SID and storing the mapped information is a basic operation of the CP 501 that uses the telephony service. The CD 502 uses the mapped information to deliver an event to selected ones of multiple CPs.

[0039] A user can invoke a 'SetFriendlyName()' action using the CP 501, or the 'Set-FriendlyName()' action can be set to be automatically invoked upon receipt of a response to the subscribe request.

[0040] According to an embodiment of the present invention, another CP device can generate a policy by collecting information on CPs that sent the subscribe request. This CP device is referred to as a policy manager 503.

[0041] In step 530, the policy manager 503 may collect the information on CPs by invoking, for example, a 'GetSIdList()' action at the CD 502. In step 535, the policy manager 503 receives a list of CP information stored in the CD 502. The information list includes mapping information between SIDs that the CD 502 assigned to individual CPs, and UUIDs and friendly names of the CPs. In step 540, the policy manager 503 generates a policy based on the received information. Based on user input, the policy manager 503 may set a CP to which a call/SMS reception event is to be delivered and a CP to which events are not to be delivered. The policy manager 503 may also set whether to perform an authentication request in response to a detailed information request for a call/SMS event from a CP, or whether to encrypt detailed event information. That is, the policy manager 503 generates an event policy by setting event delivery conditions (at least one of delivery of event information, authentication request for event information delivery, and encryption of event information) based on user input regarding each service.

[0042] In step 545, the policy manager 503 delivers the generated policy to the relevant CD 502 by invoking, for example, an 'SetCallPolicy()' action.

[0043] Thereafter, if a call event occurs in step 550 as an incoming call is received at the relevant CD 502, the CD 502 delivers the call event to the CP 501 according to the set policy in step 555.

[0044] FIG. 6 illustrates a filter-based event delivery operation during a UPnP service, according to another embodiment of the present invention. The method shown in FIG. 6 sets the policy using a variety of information in addition to the friendly name information.

[0045] Referring to FIG. 6, in step 605, a CP 601 discovers a CD 602, or the CD 602 advertises its location. In step 610, the CP 601 sends a subscribe request to a telephony service of the CD 602. In step 615, the CD 602 assigns an SID to the CP 601, accepting the subscribe request from the control point 601. In step 620, the CD 602 returns the assigned SID to the CP 601.

[0046] In step 625, the CP 601 delivers its information to the CD 602, and may deliver a user name in addition to its UUID and friendly name information. This operation may be performed by a 'SetFriendlyName()' action. A policy manager 603 sends a request for information on CPs to the CD 602 in step 630, and receives the information on CPs from the CD 602 in step 635. This operation may be performed by a 'GetSub-scribeList()' action.

[0047] In step 640, the policy manager 603 generates a policy for the CD 602, i.e., filters for event delivery, based on the information on the CP 601, which is received from the CD 602. In step 645, the policy manager 603 delivers the policy to the CD 602 using 'Set-FilterForCallNotification(FilterList) '.

[0048] If a call reception event occurs in step 650, the CD 602 generates a TLS session in step 655 and optionally delivers the event according to the set policy (filter) in step 660. In step 655, the CD 602 can generate a TLS session on the port of the callback URL that the CP 601 delivered along with the subscribe request.

[0049] Accordingly, the CD 602 may divide users based on the set policy, i.e., filter, using not only IDs and SIDs of the CPs that will receive an event, but also user names, and deliver the event to the users. Even for events that are delivered to the same user, the CD 602 may filter the events by applying a specific condition according to values of the events. In addition, the CD 602 may optionally encrypt the events according to such several conditions.

[0050] FIG. 11 is a filter list in a filter-based event delivery operation during a UPnP service, according to another embodiment of the present invention. As illustrated in FIG. 11, in 'AllowTargetList' of a filter, a 'Receiving-CallInfo' state variable transmits events to 'Mark's Game Console' with a name 'ACME Widget Model XYZ', and the event is encrypted using an encryption key with ID=0.

[0051] FIG. 7 is a diagram illustrating a detailed event delivery operation during a UPnP service, according to an embodiment of the present invention. FIG. 8 is a diagram illustrating a detailed event delivery operation when encryption parameter negotiation is not performed, according to an embodiment of the present invention.

[0052] In the processes shown in FIGs. 7 and 8, when a CP 701, 801 sends a request for detailed call/SMS information to a CD 702, 802, the CD 702, 802 requests authentication based on a policy or provides encrypted detailed information. However, in the operation disclosed in FIG. 7, the CD 702 provides a privacy (personal information) protection function in response to the detailed call/SMS information request from the CP 701 and a parameter negotiation necessary for authentication or encryption is needed.

[0053] If a call or an SMS is received at the CD 702 in step 705, the CD 702 determines occurrence of an event in step 710 and delivers the event to the CP 701 in step 715.

[0054] In step 720, the CP 701 sends a request for detailed information about the call/SMS to the CD 702. The CD 702 determines in step 725 whether to perform encryption or authentication, based on a set policy. The policy referred to in step 725 can be a policy that is set by the policy manager as described above with reference to FIGs. 5 and 6. When the CD 702 determines to perform encryption or authentication in step 725, the CD 702 returns an error code of 701 (Privacy Mode enabled) in response to the detailed call/SMS information request from the CP 701 in step 730.

[0055] If the error code value is 701, the CP 701 is authenticated by the CD 702 by receiving a password from the user in step 735, or the CP 701 performs parameter negotiation with the CD 702 necessary for encryption in step 740. Alternatively, both of steps 735 and 740 may be performed. If the CP 701 re-requests the detailed call/SMS information in step 745, the CD 702 provides the detailed call/SMS information based on the authentication result or the negotiated encryption parameters in step 750. In step 755, the CP 701 displays the provided information.

[0056] FIG. 8 illustrates a simplified operation for a case where encryption parameter negotiation is unneeded, according to an embodiment of the present invention.

[0057] Referring to FIG. 8, if a call or an SMS is received at the CD 802 in step 805, the CD 802 determines occurrence of an event in step 810 and delivers the event to the CP 801 in step 815.

[0058] In step 820, the CP 801 sends a request for detailed information about the call/SMS to the CD 802. In step 825, the CD 802 determines whether to perform encryption, based on a set policy. The policy referred to in step 825 can be a policy that is set by the policy manager as described above with reference to FIGs. 5 and 6. If the CD 802 determines to perform encryption in step 825, the CD 802 encrypts (encodes) a call/ SMS message and sends the encrypted call/SMS message to the CP 801 in step 830.

[0059] The CP 801 decrypts (decodes) the call/SMS message received from the CD 802 by receiving a password from the user in step 835, and displays the decrypted call/SMS message in step 840.

[0060] Instead of using a 'SetFriendlyName()' action in delivering information on a CP to a controlled device CD, the present invention may include such information in a subscribe request message when first making a subscribe request. FIG. 9 is a subscribe request message in which information on a CP is included in a policy-based event delivery operation during a UPnP service, according to an embodiment of the present invention.

[0061] When the control point information is delivered in the subscribe request message during sending of the

subscribe request in an embodiment of the present invention, an additional header may be defined in an event message in the UPnP Device Architecture standard. As illustrated in FIG. 9, the CP information may be described by further defining a SUBSCRIBER.UPNP.ORG header. The 'SetFriendlyName()' action in FIGs. 5 and 6 may be omitted if the CP information is delivered along with the subscribe request.

[0062] FIG. 10 is a block diagram of a device for protecting personal information during a UPnP service, according to an embodiment of the present invention. Referring to FIG. 10, a CD for privacy protection includes a receiver 1010, an event manager 1020, an authentication requester 1030, a target selector 1040, a message encryptor 1050, a transmitter 1060, an authenticated-device list information storage 1080, a policy information storage 1070, and an encryption algorithm information storage 1090. The CD communicates with a display device 1001 that serves as a CP.

[0063] The receiver 1010 receives messages and information over a home network.

[0064] The event manager 1020 determines when an event occurs, and delivers the event only to an allowed CP according to a policy stored in the policy information storage 1070. The event manager 1020 determines whether to send an authentication request to the requesting CP 1001 or to encrypt a message to be delivered to the CP 1001 according to the policy.

[0065] The authentication requester 1030 makes an authentication request based on the decision of the event manager 1020.

[0066] The message encryptor 1050 encrypts event information based on the decision of the event manager 1020.

[0067] The target selector 1040 selects a target to which it will transmit a notification for an authentication request or event information, upon request of the event manager 1020.

[0068] The transmitter 1060 transmits the notification or the event information to the CP, or the display device 1001.

[0069] The policy information storage 1070 stores policy information received from (or set by) an external policy manager (not shown). The authenticated-device list information storage 1080 stores information about authenticated CPs. The encryption algorithm information storage 1090 stores an encryption algorithm to be used for encrypting detailed call/SMS information messages.

[0070] As is apparent from the foregoing description, according to embodiments of the present invention, when an event occurs in a service that a UPnP home network system provides to a CD, the CD performs event notification based on a set policy, without delivering the event to all CP devices tha sent a subscribe request to the service. In addition, based on the set policy, the CD may request authentication or encrypt detailed event information with personal information, which is requested by the CP.

[0071] Accordingly, the present invention prevents privacy information, which is stored in the CD or provided by the CD through a service, from being included in the event information, making it possible to protect the user's personal information.

[0072] Embodiments of the present invention can also be embodied as computer-readable codes on a computer-readable recording medium. The computer-readable recording medium is any data storage device that can store data, which can thereafter be read by a computer system. Examples of computer-readable recording medium include, but are not limited to, Read-Only Memory (ROM), Random-Access Memory (RAM), CD-ROMs, magnetic tapes, floppy disks, optical data storage devices, and carrier waves (such as data transmission through the Internet via wired or wireless transmission paths). The computer-readable recording medium can also be distributed over network-coupled computer systems so that the computer-readable code is stored and executed in a distributed fashion. Also, function programs, codes, and code segments for accomplishing the present invention can be easily construed as within the scope of the invention by programmers skilled in the art to which the present invention pertains.

[0073] While the invention has been shown and described with reference to certain embodiments thereof, it will be understood by those skilled in the art that various changes in form and detail may be made therein without departing from the scope of the invention as defined by the appended claims.

Claims

1. A method for protecting personal information in a home network, the method comprising the steps of:

receiving (510), by a controlled device (502), a subscribe request for a service of the controlled device, from a control point (501);
accepting, by the controlled device (502), the subscribe request;
receiving (525), by the controlled device (502), information about the control point (501) from the control point (501); and
performing (555), by the controlled device (502), event information delivery to the control point (501) according to a policy when an event occurs in the controlled device (502);
wherein the method is **characterized in that** it further comprises the steps of:

transmitting (535), by the controlled device (502), the information about the control point (501) to a policy manager (503); and
receiving (545), by the controlled device (502), a policy for event information delivery to the control point (501), which is generated

by the policy manager (503) based on the information about the control point (501);
wherein the step of performing (555), by the controlled device (502), event information delivery to the control point (501) is in accordance with the policy received from the policy manager (503),
wherein the policy manager generates the policy for event information delivery by setting event delivery conditions based on user input, said event delivery conditions prescribing whether at least one of delivery, authentication and encryption is to be applied.

2. The method of claim 1, wherein accepting the subscribe request comprises assigning (515), by the controlled device (502), a Subscription Identifier, SID, in response to the subscribe request and delivering (520) the assigned SID to the control point (501).

3. The method of claim 1, wherein the information about the control point (501) comprises a Universally Unique Identifier, UUID, and a friendly name of the control point (501).

4. The method of claim 2, wherein receiving (525) information comprises receiving, by the controlled device (502), information about the control point (501), which is mapped to the assigned SID, from the control point (501).

5. The method of claim 1, further comprising:

collecting (530), by the policy manager (503), the information about the control point (501);
generating (540), by the policy manager (503), the policy for event information delivery to the control point (501) based on the collected information about the control point (50); and
delivering (545), by the policy manager (503), the generated policy to the controlled device (502).

6. The method of claim 5, wherein the information about the control point (501) further comprises a user name.

7. The method of claim 1, wherein the information about the control point (501) is included in the subscribe request message.

8. The method of claim 1, further comprising:

sending, by the control point (501), a request for detailed information about an event to the controlled device (502) upon receiving the event;
determining, by the controlled device (502), whether to encrypt the detailed information about the event, based on the policy; and
encrypting, by the controlled device (502), the detailed information about the event and transmitting the encrypted information to the control point (501), when the controlled device (502) determines to encrypt the detailed information about the event based on the policy.

9. The method of claim 8, wherein determining whether to encrypt the detailed information comprises:

determining, by the controlled device (502), whether to encrypt detailed information about the event and whether to authenticate the control point (501), based on the policy; and
receiving, by the controlled device (502), a password from a user of the control point (501) and performing authentication using the password, when the controlled device (502) determines to authenticate the control point (501) based on the policy.

10. A controlled device (502) for protecting personal information in a home network, the controlled device (502) comprising:

a receiver (1010);
an event manager (1020); and
a transmitter (1060) ;
wherein the receiver (1010) is arranged to receive (510) information over the home network including a subscribe request for a service of the controlled device from a control point (501);
wherein the controlled device (502) is arranged to accept the subscribe request;
wherein the receiver (1010) is further arranged to receive (525) information about the control point from the control point (501);
wherein the event manager (1020) is arranged to determine when an event occurs and to control event information delivery to the control point (501) according to a policy; and
wherein the transmitter (1060) is arranged to transmit (555) the event information to the control point (501);
wherein the controlled device is **characterized in that**:

the transmitter (1060) is further arranged to transmit (535) the information about the control point (501) to a policy manager (503);
the receiver (1010) is further arranged to receive (545) a policy for event information delivery to the control point (501), which is generated by a policy manager (503) based on the information about the control point

(501); and
the event manager (1020) is further arranged to control event information delivery to the control point (501) according to the policy received from the policy manager (503),
wherein the policy manager generates the policy for event information delivery by setting event delivery conditions based on user input, said event delivery conditions prescribing whether at least one of delivery, authentication and encryption is to be applied.

11. The controlled device of claim 10, further comprising:

an authentication requester (1030);
a message encryptor (1050);
a target selector (1040) arranged to select a target to which the event information is to be transmitted;
a policy information storage (1070) arranged to store the policy received from a policy manager (503);
an encryption algorithm information storage (1090) arranged to store an encryption algorithm to be used for the encryption of the event information; and
an authenticated-device list information storage (1080) arranged to store a list of authenticated control points (501);
wherein the event manager (1020) is further arranged to decide whether to send an authentication request to the control point (501) or to encrypt the event information to be delivered to the control point (501) based on the policy;
wherein the authentication requester (1030) is arranged to make an authentication request based on the decision of the event manager (1020); and
wherein the message encryptor (1050) is arranged to encrypt the event information based on the decision of the event manager (1020).

12. A home network comprising:

the controlled device (501) of claim 10 or claim 11; and
a control point (501) for protecting personal information in a home network, the control point (501) comprising:

means for sending (510) a subscribe request for a service of a controlled device (502);
means for performing authentication with the controlled device (502); and
means for receiving (555) event information for an occurred event delivered from a controlled device (502) through a TLS session between the control point (501) and the controlled device (502);
wherein the TLS session is generated by the controlled device (502) when the event occurs in the controlled device (502).

13. The home network of claim 12, wherein the means for performing authentication is further arranged to generate the TLS session using a self-signed certificate for channel protection between the control point (501) and the controlled device (502), and to perform an authentication procedure using an introduction protocol.

14. The home network of claim 12, further comprising:

means for including information about a port of a callback Uniform Resource Locator, URL in a message for the subscribe request when sending the subscribe request; and
means for generating the TLS session on the port of the callback URL, when the event occurs in the controlled device (502).

Patentansprüche

1. Verfahren zum Schutz von persönlichen Informationen in einem Heimnetzwerk, wobei das Verfahren folgende Schritte umfasst:

Empfangen (510), durch eine gesteuerte Vorrichtung (502), einer Abonnement-Anfrage nach einem Dienst der gesteuerten Vorrichtung von einem Kontrollpunkt (501);
Annehmen, durch die gesteuerte Vorrichtung (502), der Abonnement-Anfrage;
Empfangen (525), durch die gesteuerte Vorrichtung (502), von Informationen über den Kontrollpunkt (501) von dem Kontrollpunkt (501); und
Durchführen (555), durch die gesteuerte Vorrichtung (502), einer Lieferung von Ereignisinformationen an den Kontrollpunkt (501) gemäß einer Richtlinie, wenn ein Ereignis in der gesteuerten Vorrichtung (502) auftritt;
wobei das Verfahren **dadurch gekennzeichnet ist, dass** es ferner folgende Schritte umfasst:

Senden (535), durch die gesteuerte Vorrichtung (502), der Informationen über den Kontrollpunkt (501) zu einem Richtlinienmanager (503); und
Empfangen (545), durch die gesteuerte Vorrichtung (502), einer Richtlinie für die Lieferung von Ereignisinformationen an den Kontrollpunkt (501), die von dem Richtlinienmanager (503) basierend auf den In-

formationen über den Kontrollpunkt (501) erzeugt wird;
wobei der Schritt der Durchführung (555), durch die gesteuerte Vorrichtung (502), der Lieferung von Ereignisinformationen an den Kontrollpunkt (501) der Richtlinie entspricht, die von dem Richtlinienmanager (503) empfangen wird,
wobei der Richtlinienmanager die Richtlinie für die Lieferung von Ereignisinformationen durch Einstellen der Ereignislieferbedingungen basierend auf einer Benutzereingabe erzeugt, wobei die Ereignislieferbedingungen vorschreiben, ob mindestens eine Lieferung, Authentifizierung oder Verschlüsselung angewendet werden soll.

2. Verfahren nach Anspruch 1, wobei die Annahme der Abonnement-Anfrage Folgendes umfasst: Zuweisen (515), durch die gesteuerte Vorrichtung (502), einer Abonnement-Kennung (Subscription Identifier - SID) als Reaktion auf die Abonnement-Anfrage und Lieferung (520) der zugeordneten SID an den Kontrollpunkt (501).

3. Verfahren nach Anspruch 1, wobei die Informationen über den Kontrollpunkt (501) eine universell eindeutige Kennung (Universally Unique Identifier - UUID) und einen freundlichen Namen des Kontrollpunktes (501) umfassen.

4. Verfahren nach Anspruch 2, wobei das Empfangen (525) der Informationen das Empfangen, durch die gesteuerte Vorrichtung (502), von Informationen über den Kontrollpunkt (501) umfasst, die der zugeordneten SID von dem Kontrollpunkt (501) zugeordnet sind.

5. Verfahren nach Anspruch 1, das ferner Folgendes umfasst:

Sammeln (530), durch den Richtlinienmanager (503), der Informationen über den Kontrollpunkt (501);
Erzeugen (540), durch den Richtlinienmanager (503), der Richtlinie für die Lieferung von Ereignisinformationen an den Kontrollpunkt (501) basierend auf den gesammelten Informationen über den Kontrollpunkt (50);
Liefern (545), durch den Richtlinienmanager (503), der erzeugten Richtlinie an die gesteuerte Vorrichtung (502).

6. Verfahren nach Anspruch 5, wobei die Informationen über den Kontrollpunkt (501) ferner einen Benutzernamen umfassen.

7. Verfahren nach Anspruch 1, wobei die Informationen über den Kontrollpunkt (501) in der Abonnement-Anfragenachricht enthalten sind.

8. Verfahren nach Anspruch 1, das ferner Folgendes umfasst:

Senden, durch den Kontrollpunkt (501), einer Anfrage nach ausführlichen Informationen über ein Ereignis zu der gesteuerten Vorrichtung (502) bei Empfang des Ereignisses;
Bestimmen basierend auf der Richtlinie, durch die gesteuerte Vorrichtung (502), ob die ausführlichen Informationen über das Ereignis verschlüsselt werden sollen; und
Verschlüsseln, durch die gesteuerte Vorrichtung (502), der ausführlichen Informationen über das Ereignis und Übertragen der verschlüsselten Informationen zu dem Kontrollpunkt (501), wenn die gesteuerte Vorrichtung (502) basierend auf der Richtlinie bestimmt, die ausführlichen Informationen über das Ereignis zu verschlüsseln.

9. Verfahren nach Anspruch 8, wobei das Bestimmen, ob die ausführlichen Informationen verschlüsselt werden sollen, Folgendes umfasst:

Bestimmen basierend auf der Richtlinie, durch die gesteuerte Vorrichtung (502), ob die ausführlichen Informationen über das Ereignis verschlüsselt werden sollen und ob der Kontrollpunkt (501) authentifiziert werden soll; und
Empfangen, durch die gesteuerte Vorrichtung (502), eines Passworts von einem Benutzer des Kontrollpunkts (501) und Durchführen einer Authentifizierung unter Verwendung des Passworts, wenn die gesteuerte Vorrichtung (502) basierend auf der Richtlinie bestimmt, den Kontrollpunkt (501) zu authentifizieren.

10. Gesteuerte Vorrichtung (502) zum Schutz von persönlichen Informationen in einem Heimnetzwerk, wobei die gesteuerte Vorrichtung (502) Folgendes umfasst:

einen Empfänger (1010);
einen Ereignismanager (1020); und
einen Sender (1060);
wobei der Empfänger (1010) dafür ausgelegt ist, Informationen über das Heimnetzwerk zu empfangen (510), die eine Abonnement-Anfrage nach einem Dienst der gesteuerten Vorrichtung von einem Kontrollpunkt (501) umfassen;
wobei die gesteuerte Vorrichtung (502) dafür ausgelegt ist, die Abonnement-Anfrage zu akzeptieren;
wobei der Empfänger (1010) ferner dafür ausgelegt ist, Informationen über den Kontrollpunkt

von dem Kontrollpunkt (501) zu empfangen (525);
wobei der Ereignismanager (1020) für Folgendes ausgelegt ist: Bestimmen, wann ein Ereignis stattfindet, und Steuern der Lieferung der Ereignisinformationen an den Kontrollpunkt (501) gemäß einer Richtlinie; und
wobei der Sender (1060) dafür ausgelegt ist, die Ereignisinformation zu dem Kontrollpunkt (501) zu senden (555);
wobei die gesteuerte Vorrichtung **dadurch gekennzeichnet ist, dass**:

der Sender (1060) ferner dafür ausgelegt ist, die Informationen über den Kontrollpunkt (501) zu einem Richtlinienmanager (503) zu senden (535);
der Empfänger (1010) ferner dafür ausgelegt ist, eine Richtlinie für die Lieferung von Ereignisinformationen an den Kontrollpunkt (501) zu empfangen (545), die von einem Richtlinienmanager (503) basierend auf den Informationen über den Kontrollpunkt (501) erzeugt wird; und
der Ereignismanager (1020) ferner dafür ausgelegt ist, die Lieferung von Ereignisinformationen an den Kontrollpunkt (501) gemäß der Richtlinie, die von dem Richtlinienmanager (503) empfangen wird, zu steuern,
wobei der Richtlinienmanager die Richtlinie für die Lieferung von Ereignisinformationen durch Einstellen der Ereignislieferbedingungen basierend auf einer Benutzereingabe erzeugt, wobei die Ereignislieferbedingungen vorschreiben, ob mindestens eine Lieferung, Authentifizierung oder Verschlüsselung angewendet werden soll.

11. Gesteuerte Vorrichtung nach Anspruch 10, die ferner Folgendes umfasst:

einen Authentifizierungsanforderer (1030);
einen Nachrichtenverschlüssler (1050);
eine Zielwählvorrichtung (1040), die dafür ausgelegt ist, ein Ziel zu wählen, zu dem die Ereignisinformationen zu übertragen sind;
einen Richtliniendatenspeicher (1070), der dafür ausgelegt ist, die Richtlinie zu speichern, die von einem Richtlinienmanager (503) empfangen wurde;
einen Verschlüsselungsalgorithmusdatenspeicher (1090) der dafür ausgelegt ist, einen Verschlüsselungsalgorithmus zu speichern, der für die Verschlüsselung der Ereignisinformationen zu verwenden ist; und
einen Listendatenspeicher (1080) für authentifizierte Vorrichtungen, der dafür ausgelegt ist, eine Liste von authentifizierten Kontrollpunkten zu speichern (501);
wobei der Ereignismanager (1020) ferner für Folgendes ausgelegt ist: Entscheiden basierend auf der Richtlinie, ob eine Authentifizierungsanforderung an den Kontrollpunkt (501) zu senden ist oder ob die Ereignisinformationen, die zu dem Kontollpunkt (501) zu senden sind, zu verschlüsseln sind;
wobei der Authentifizierungsanforderer (1030) dafür ausgelegt ist, eine Authentifizierungsanforderung basierend auf der Entscheidung des Ereignismanagers (1020) zu stellen; und
wobei der Nachrichtenverschlüssler (1050) dafür ausgelegt ist, die Ereignisinformationen basierend auf der Entscheidung des Ereignismanagers (1020) zu verschlüsseln.

12. Heimnetzwerk, das Folgendes umfasst:

die gesteuerte Vorrichtung (501) nach Anspruch 10 oder Anspruch 11; und
einen Kontrollpunkt (501) zum Schutz von persönlichen Informationen in einem Heimnetzwerk, wobei der Kontrollpunkt (501) Folgendes umfasst:

Mittel (510) zum Senden einer Abonnement-Anfrage nach einem Dienst einer gesteuerten Vorrichtung (502);
Mittel zur Durchführung einer Authentifizierung mit der gesteuerten Vorrichtung (502); und
Mittel (555) zum Empfangen von Ereignisinformationen für ein aufgetretenes Ereignis, das von einer gesteuerten Vorrichtung (502) durch eine TLS-Sitzung zwischen dem Kontrollpunkt (501) und der gesteuerten Vorrichtung (502) geliefert wird;
wobei die TLS-Sitzung von der gesteuerten Vorrichtung (502) erzeugt wird, wenn das Ereignis in der gesteuerten Vorrichtung (502) auftritt.

13. Heimnetzwerk nach Anspruch 12, wobei das Mittel zur Durchführung der Authentifizierung ferner für Folgendes ausgelegt ist: Erzeugen der TLS-Sitzung unter Verwendung eines selbst signierten Zertifikats für den Kanalschutz zwischen dem Kontrollpunkt (501) und der gesteuerten Vorrichtung (502) und Durchführen eines Authentifizierungsverfahrens unter Verwendung eines Einführungsprotokolls.

14. Heimnetzwerk nach Anspruch 12, das ferner Folgendes umfasst:

Mittel zum Einschließen von Informationen über einen Port eines Callback-Uniform Resource Locators, URL, in einer Nachricht für die Abon-

nement-Anforderung, wenn die Abonnement-Anforderung gesendet wird; und
Mittel zum Erzeugen der TLS-Sitzung auf dem Port der Callback-URL, wenn das Ereignis in der gesteuerten Vorrichtung (502) auftritt.

Revendications

1. Un procédé de protection d'informations personnelles dans un réseau domestique, le procédé comprenant les opérations suivantes :

la réception (510), par un dispositif commandé (502), d'une demande d'abonnement pour un service du dispositif commandé, à partir d'un point de commande (501),
l'acceptation, par le dispositif commandé (502), de la demande d'abonnement,
la réception (525), par le dispositif commandé (502), d'informations relatives au point de commande (501) à partir du point de commande (501), et
l'exécution (555), par le dispositif commandé (502), d'une remise d'informations d'événement au point de commande (501) en fonction d'une règle lorsqu'un événement se produit dans le dispositif commandé (502),
où le procédé est **caractérisé en ce qu'**il comprend en outre les opérations suivantes :

la transmission (535), par le dispositif commandé (502), des informations relatives au point de commande (501) à un gestionnaire de règles (503), et
la réception (545), par le dispositif commandé (502), d'une règle pour une remise d'informations d'événement au point de commande (501) qui est générée par le gestionnaire de règles (503) en fonction des informations relatives au point de commande (501),
où l'opération d'exécution (555), par le dispositif commandé (502), d'une remise d'informations d'événement au point de commande (501) est conforme à la règle reçue du gestionnaire de règles (503),
où le gestionnaire de règles génère la règle pour une remise d'informations d'événement par la définition de conditions de remise d'événement en fonction d'une entrée d'utilisateur, lesdits conditions de remise d'événement prescrivant si au moins une opération parmi remise, authentification et chiffrement doit être appliquée.

2. Le procédé selon la Revendication 1, où l'acceptation de la demande d'abonnement comprend l'attribution (515), par le dispositif commandé (502), d'un identifiant d'abonnement, SID, en réponse à la demande d'abonnement et la remise (520) du SID attribué au point de commande (501).

3. Le procédé selon la Revendication 1, où les informations relatives au point de commande (501) comprennent un identifiant universellement unique, UUID, et un nom convivial du point de commande (501).

4. Le procédé selon la Revendication 2, où la réception (525) d'informations comprend la réception, par le dispositif commandé (502), d'informations relatives au point de commande (501), qui sont mises en correspondance avec le SID attribué, à partir du point de commande (501).

5. Le procédé selon la Revendication 1, comprenant en outre :

le recueil (530), par le gestionnaire de règles (503), des informations relatives au point de commande (501),
la génération (540), par le gestionnaire de règles (503), de la règle de remise d'informations d'événement au point de commande (501) en fonction des informations recueillies relatives au point de commande (50), et
la remise (545), par le gestionnaire de règles (503), de la règle générée au dispositif commandé (502).

6. Le procédé selon la Revendication 5, où les informations relatives au point de commande (501) comprennent en outre un nom d'utilisateur.

7. Le procédé selon la Revendication 1, où les informations relatives au point de commande (501) sont incluses dans le message de demande d'abonnement.

8. Le procédé selon la Revendication 1, comprenant en outre :

l'envoi, par le point de commande (501), d'une demande d'informations détaillées relatives à un événement au dispositif commandé (502) après la réception de l'événement,
la détermination, par le dispositif commandé (502), s'il convient de chiffrer les informations détaillées relatives à l'événement en fonction de la règle, et
le chiffrement, par le dispositif commandé (502), des informations détaillées relatives à l'événement et la transmission des informations chiffrées au point de commande (501) lorsque le dispositif commandé (502) détermine qu'il con-

vient de chiffrer les informations détaillées relatives à l'événement en fonction de la règle.

9. Le procédé selon la Revendication 8, où la détermination s'il convient de chiffrer les informations détaillées comprend :

la détermination, par le dispositif commandé (502), s'il convient de chiffrer les informations détaillées relatives à l'événement et s'il convient d'authentifier le point de commande (501) en fonction de la règle, et
la réception, par le dispositif commandé (502), d'un mot de passe à partir d'un utilisateur du point de commande (501) et l'exécution d'une authentification au moyen du mot de passe lorsque le dispositif commandé (502) détermine qu'il convient d'authentifier le point de commande (501) en fonction de la règle.

10. Un dispositif commandé (502) de protection d'informations personnelles dans un réseau domestique, le dispositif commandé (502) comprenant :

un récepteur (1010),
un gestionnaire d'événements (1020), et
un émetteur (1060),
où le récepteur (1010) est agencé de façon à recevoir (510) des informations par l'intermédiaire du réseau domestique comprenant une demande d'abonnement pour un service du dispositif commandé à partir d'un point de commande (501),
où le dispositif commandé (502) est agencé de façon à accepter la demande d'abonnement,
où le récepteur (1010) est agencé en outre de façon à recevoir (525) des informations relatives au point de commande à partir du point de commande (501),
où le gestionnaire d'événements (1020) est agencé de façon à déterminer le moment où un événement se produit et à commander une remise d'informations d'événement au point de commande (501) en fonction d'une règle, et
où l'émetteur (1060) est agencé de façon à transmettre (555) les informations d'événement au point de commande (501),
où le dispositif commandé est **caractérisé en ce que** :

l'émetteur (1060) est agencé en outre de façon à transmettre (535) les informations relatives au point de commande (501) à un gestionnaire de règles (503),
le récepteur (1010) est agencé en outre de façon à recevoir (545) une règle de remise d'informations d'événement au point de commande (501) qui est générée par un gestionnaire de règles (503) en fonction des informations relatives au point de commande (501), et
le gestionnaire d'événements (1020) est agencé en outre de façon à commander une remise d'informations d'événement au point de commande (501) en fonction de la règle reçue du gestionnaire de règles (503), où le gestionnaire de règles génère la règle de remise d'informations d'événement par la définition de conditions de remise d'événement en fonction d'une entrée d'utilisateur, lesdits conditions de remise d'événement prescrivant si au moins une opération parmi remise, authentification et chiffrement doit être appliquée.

11. Le dispositif commandé selon la Revendication 10, comprenant en outre :

un demandeur d'authentification (1030),
un chiffreur de messages (1050),
un sélecteur de cible (1040) agencé de façon à sélectionner une cible à laquelle les informations d'événement doivent être transmises,
un espace mémoire d'informations de règle (1070) agencé de façon à conserver en mémoire la règle reçue d'un gestionnaire de règles (503),
un espace mémoire d'informations d'algorithme de chiffrement (1090) agencé de façon à conserver en mémoire un algorithme de chiffrement destiné à être utilisé pour le chiffrement des informations d'événement, et
un espace mémoire d'informations de liste de dispositifs authentifiés (1080) agencé de façon à conserver en mémoire un liste de points de commande authentifiés (501),
où le gestionnaire d'événements (1020) est agencé en outre de façon à décider s'il convient d'envoyer une demande d'authentification au point de commande (501) ou de chiffrer les informations d'événement à remettre au point de commande (501) en fonction de la règle,
où le demandeur d'authentification (1030) est agencé de façon à effectuer une demande d'authentification en fonction de la décision du gestionnaire d'événements (1020), et
où le chiffreur de messages (1050) est agencé de façon à chiffrer les informations d'événement en fonction de la décision du gestionnaire d'événements (1020).

12. Un réseau domestique comprenant :

le dispositif commandé (501) selon la Revendication 10 ou 11, et
un point de commande (501) destiné à la protection d'informations personnelles dans un ré-

seau domestique, le point de commande (501) comprenant :

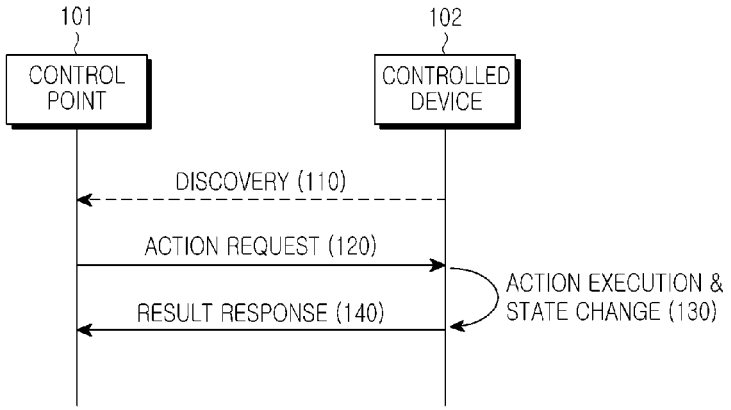
un moyen d'envoi (510) d'une demande d'abonnement pour un service d'un dispositif commandé (502),
un moyen d'exécution d'une authentification avec le dispositif commandé (502), et
un moyen de réception (555) d'informations d'événement pour un événement survenu remises à partir d'un dispositif commandé (502) par l'intermédiaire d'une session TLS entre le point de commande (501) et le dispositif commandé (502),
où la session TLS est générée par le dispositif commandé (502) lorsque l'événement se produit dans le dispositif commandé (502).

13. Le réseau domestique selon la Revendication 12, où le moyen d'exécution d'une authentification est agencé en outre de façon à générer la session TLS au moyen d'un certificat auto-signé pour une protection de canal entre le point de commande (501) et le dispositif commandé (502) et à exécuter une procédure d'authentification au moyen d'un protocole d'introduction.

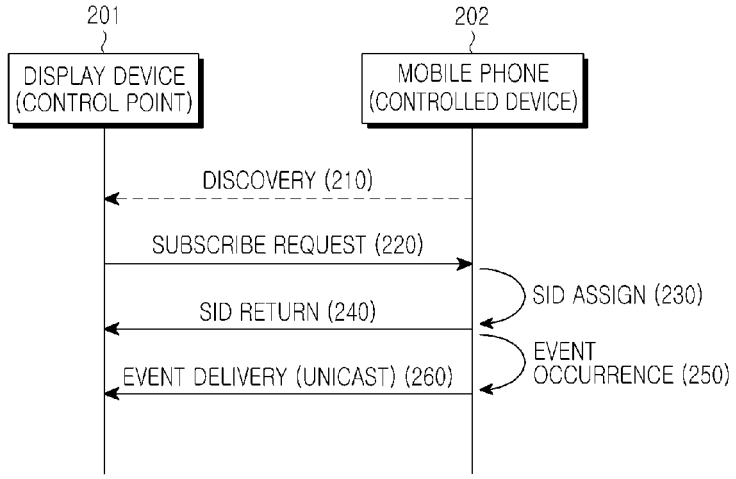
14. Le réseau domestique selon la Revendication 12, comprenant en outre :

un moyen d'inclusion d'informations relatives à un port d'un localisateur de ressources universel, URL, de rappel dans un message de demande d'abonnement lors de l'envoi de la demande d'abonnement, et
un moyen de génération de la session TLS sur le port de l'URL de rappel lorsque l'événement se produit dans le dispositif commandé (502).

[Fig. 1]



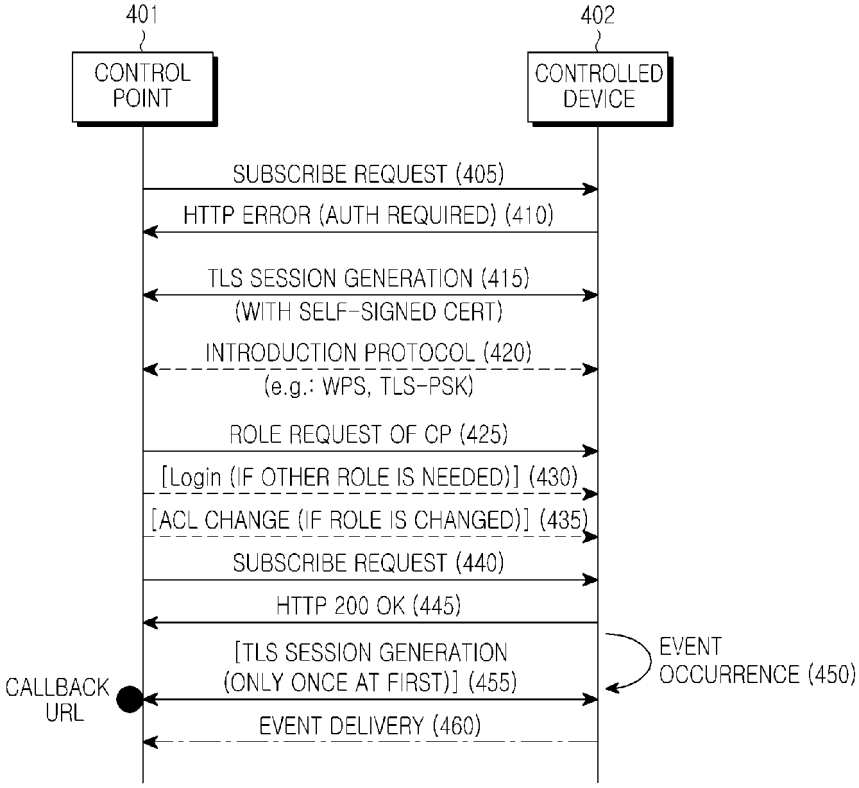
[Fig. 2]



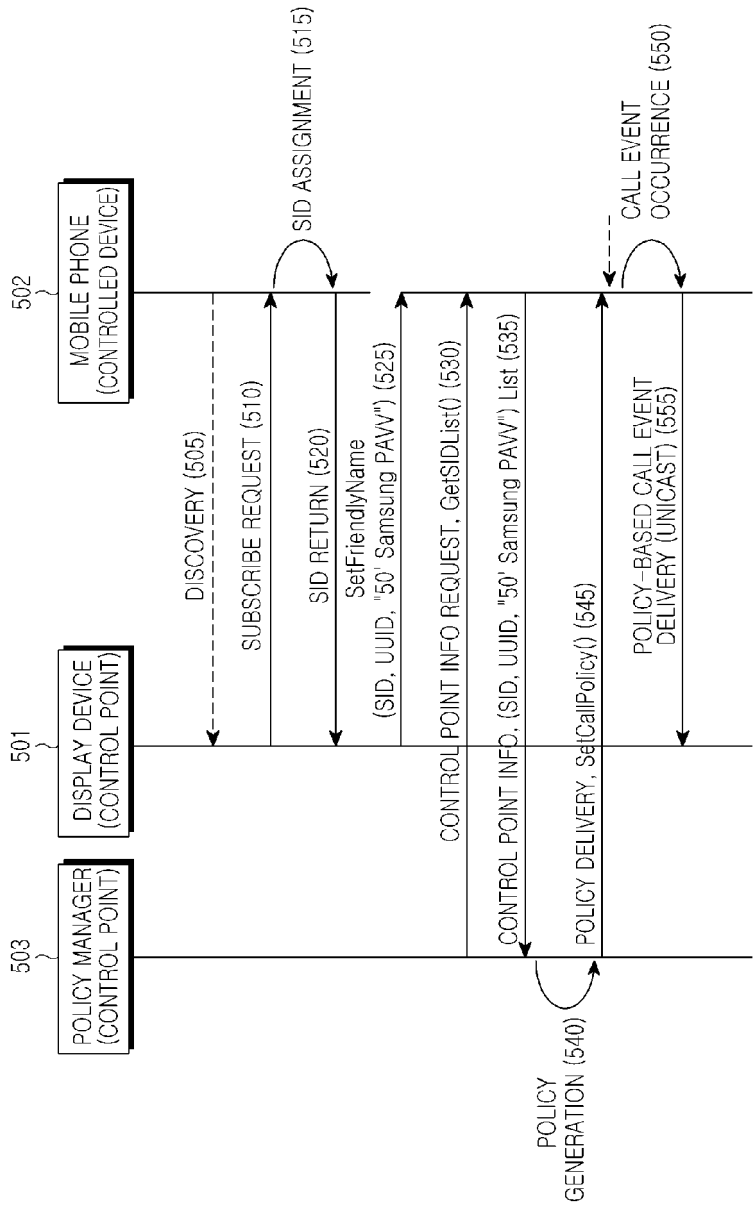
[Fig. 3]

SUBSCRIBE publisher path HTTP/1.1
HOST: publisher host:publisher port
USER-AGENT: OS/version UPnP/1.1 product/version
CALLBACK: <delivery URI>
NT: upnp : event
TIMEOUT: Second-requested subscription duration

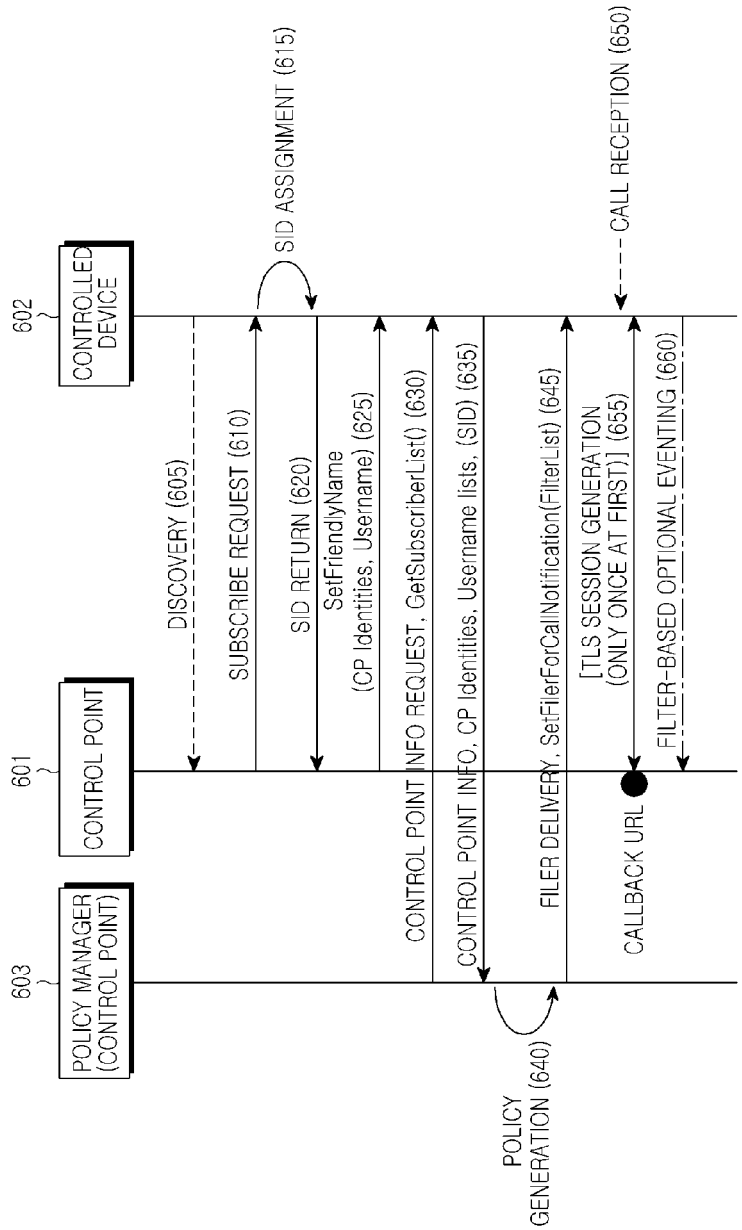
[Fig. 4]


401
402
CONTROL POINT
CONTROLLED DEVICE
SUBSCRIBE REQUEST (405)
HTTP ERROR (AUTH REQUIRED) (410)
TLS SESSION GENERATION (415)
(WITH SELF-SIGNED CERT)
INTRODUCTION PROTOCOL (420)
(e.g.: WPS, TLS-PSK)
ROLE REQUEST OF CP (425)
[Login (IF OTHER ROLE IS NEEDED)] (430)
[ACL CHANGE (IF ROLE IS CHANGED)] (435)
SUBSCRIBE REQUEST (440)
HTTP 200 OK (445)
EVENT OCCURRENCE (450)
[TLS SESSION GENERATION (ONLY ONCE AT FIRST)] (455)
CALLBACK URL
EVENT DELIVERY (460)

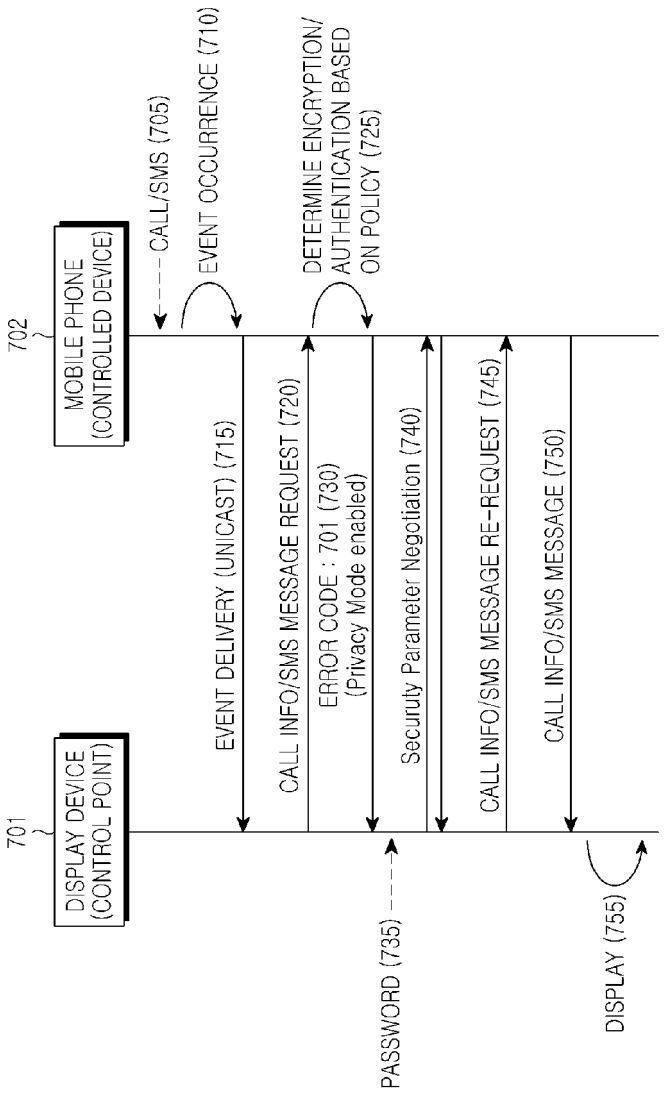
[Fig. 5]


502
MOBILE PHONE
(CONTROLLED DEVICE)
501
DISPLAY DEVICE
(CONTROL POINT)
503
POLICY MANAGER
(CONTROL POINT)
SID ASSIGNMENT (515)
CALL EVENT
OCCURRENCE (550)
DISCOVERY (505)
SUBSCRIBE REQUEST (510)
SID RETURN (520)
SetFriendlyName
(SID, UUID, "50' Samsung PAVV") (525)
CONTROL POINT INFO REQUEST, GetSIDList() (530)
CONTROL POINT INFO, (SID, UUID, "50' Samsung PAVV") List (535)
POLICY DELIVERY, SetCallPolicy() (545)
POLICY-BASED CALL EVENT
DELIVERY (UNICAST) (555)
POLICY
GENERATION (540)

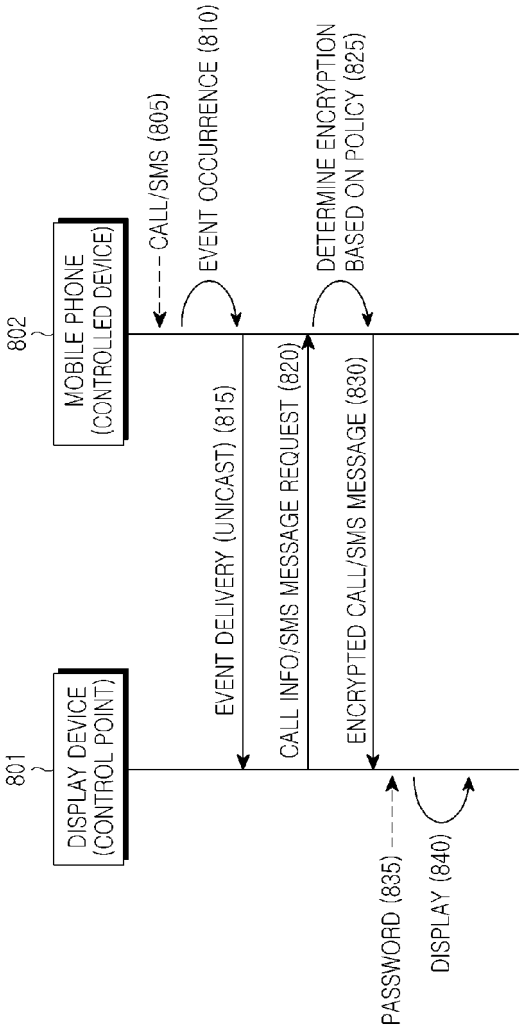
[Fig. 6]


602
CONTROLLED DEVICE
601
CONTROL POINT
603
POLICY MANAGER (CONTROL POINT)
SID ASSIGNMENT (615)
CALL RECEPTION (650)
DISCOVERY (605)
SUBSCRIBE REQUEST (610)
SID RETURN (620)
SetFriendlyName (CP Identities, Username) (625)
CONTROL POINT INFO REQUEST, GetSubscriberList() (630)
CONTROL POINT INFO, CP Identities, Username lists, (SID) (635)
FILER DELIVERY, SetFilerForCallNotification(FilterList) (645)
[TLS SESSION GENERATION (ONLY ONCE AT FIRST)] (655)
CALLBACK URL
FILTER-BASED OPTIONAL EVENTING (660)
POLICY GENERATION (640)

[Fig. 7]


MOBILE PHONE
(CONTROLLED DEVICE)
702
DISPLAY DEVICE
(CONTROL POINT)
701
CALL/SMS (705)
EVENT OCCURRENCE (710)
DETERMINE ENCRYPTION/
AUTHENTICATION BASED
ON POLICY (725)
EVENT DELIVERY (UNICAST) (715)
CALL INFO/SMS MESSAGE REQUEST (720)
ERROR CODE : 701 (730)
(Privacy Mode enabled)
Securuty Parameter Negotiation (740)
CALL INFO/SMS MESSAGE RE-REQUEST (745)
CALL INFO/SMS MESSAGE (750)
PASSWORD (735)
DISPLAY (755)

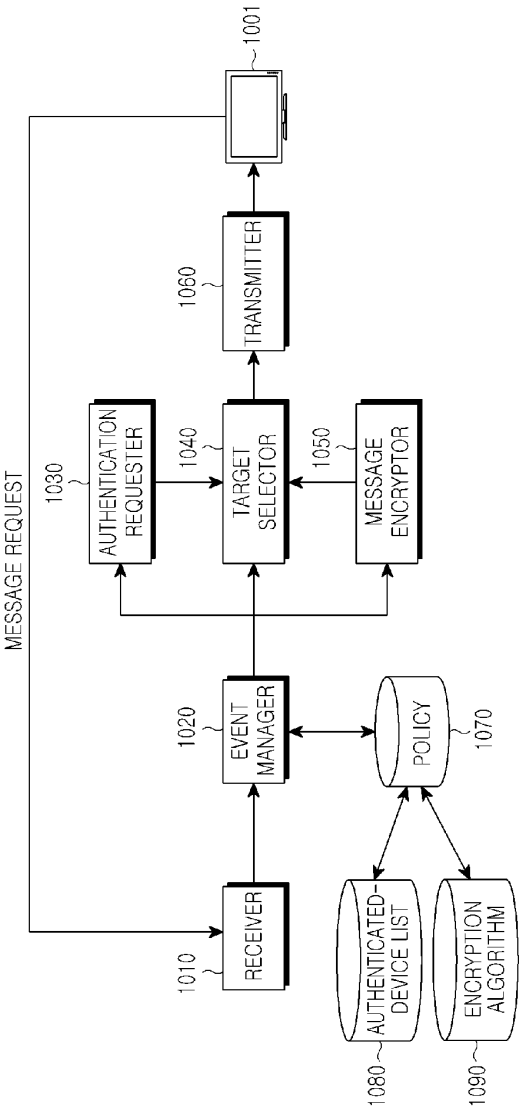
[Fig. 8]



[Fig. 9]

```
SUBSCRIBE publisher path HTTP/1.1
HOST: publisher host:publisher port
USER-AGENT: OS/version UPnP/1.1 product/version
CALLBACK: <delivery URI>
NT: upnp : event
TIMEOUT: Second-requested subscription duration
SUBSCRIBER.UPNP.ORG: uuid of CP, friendly name of the CP
```

[Fig. 10]



[Fig. 11]

```
<FilterList>
    <ServiceId>urn:upnp-org:serviceId:TS:1</ServiceId>
    <EventingStateVariable>
        <Name>ReceivingCallInfo</Name>
        <AllowTargetList>
            <CP Encrypt="Yes" EncryptKeyID=0>
                <Name>ACME Widget  Model XYZ</Name>
                <Alias>Mark's Game Console</Alias>
                <Hash>TMzI2OzM0NTueYgi93Q==</Hash>
            </CP>
        </AllowTargetList>
        <DenyTargetList>
            <User>Tom</User>
        </DenyTargetList>
    </EventingStateVariable>
</FilterList>
```

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 2005074018 A1 **[0021]**
- US 2004064575 A1 **[0022]**

Non-patent literature cited in the description

- Service-Oriented Device Communications Using the Devices Profile for Web services. **JAMMES F et al.** 21st International Conference on Advanced Information Networking and Applications Workshops. IEEE, 21 May 2007 **[0020]**
- Services and Policies for Care At Home. **FENG WANG et al.** Pervasive Health Conference and Workshops. IEEE, 01 November 2006 **[0023]**